Subquantum Information and Computation[1]

Antony Valentini[2]

Theoretical Physics Group, Blackett Laboratory, Imperial College, Prince Consort Road, London SW7 2BZ, England.[3]
Center for Gravitational Physics and Geometry, Department of Physics, The Pennsylvania State University, University Park, PA 16802, USA.
Augustus College, 14 Augustus Road, London SW19 6LN, England.[4]

It is argued that immense physical resources – for nonlocal communication, espionage, and parallel computation – are hidden from us by a veil of quantum noise that is not fundamental, but merely reflects the statistical properties of an equilibrium state in which the universe happens to be at the present time. It is suggested that 'non-quantum' or nonequilibrium matter might exist today in the form of relic particles from the early universe. We describe how such matter could be detected and put to practical use. Nonequilibrium matter could be used to send instantaneous signals, to violate the uncertainty principle, to distinguish non-orthogonal quantum states without disturbing them, to eavesdrop on quantum key distribution, and to read all the results of a parallel quantum computation.

[1]To appear in: *Proceedings of the Second Winter Institute on Foundations of Quantum Theory and Quantum Optics: Quantum Information Processing*, ed. R. Ghosh (Indian Academy of Science, Bangalore, 2002).
[2]email: a.valentini@ic.ac.uk
[3]Corresponding address.
[4]Permanent address.

1 Introduction and Motivation

In quantum theory the Born probability rule is regarded as a fundamental law of Nature: a system with wavefunction ψ has an associated probability distribution $\rho = |\psi|^2$. However, there are reasons to believe that this distribution is not fundamental, but merely corresponds to a special 'equilibrium' state, analogous to thermal equilibrium [1–7].

For there seems to be a 'conspiracy' in the known laws of physics: long-distance quantum correlations suggest that our universe is fundamentally nonlocal, and yet the nonlocality cannot be used for practical instantaneous signalling.[5] It is as if there is something nonlocal going on behind the scenes, which is hidden from us by a veil of uncertainty noise. This apparent conspiracy may be explained if one supposes that, for ensembles with a distribution $\rho = |\psi|^2$, nonlocality just *happens* to be hidden by quantum noise; while for a general distribution $\rho \neq |\psi|^2$, nonlocality would be directly visible. In other words, $\rho = |\psi|^2$ is a special state, with properties that are contingent and not fundamental.

This view suggests that while $\rho = |\psi|^2$ to high accuracy now (for all systems probed so far), this need not have been the case in the remote past: perhaps $\rho \neq |\psi|^2$ in the early universe, the relaxation $\rho \to |\psi|^2$ having taken place soon after the big bang.

A suggestive, heuristic analogy may be drawn with physics in a universe that has reached a state of thermal 'heat death', in which all systems have the same temperature [2]. In such a universe there is a universal probability distribution given by the Boltzmann rule $\rho = e^{-E/kT}/Z$, analogous to our universal Born rule $\rho = |\psi|^2$; all systems are subject to a universal thermal noise, analogous to our universal uncertainty noise; and it is impossible to convert thermal energy into useful work, just as it is impossible in our universe to convert quantum nonlocality into a useful instantaneous signal.

On this view, an analogue of the classical thermodynamic heat death has actually occurred in our universe. The apparent conspiracy between relativity and quantum theory is then explained: our experience happens to be restricted to an equilibrium state $\rho = |\psi|^2$ in which locality and uncertainty *appear* to be fundamental.

The view that our universe is in an equilibrium state may also be supported by arguments from quantum field theory in curved spacetime, where quantum and thermal fluctuations are intimately related [9]. Indeed, on this basis it has been argued that quantum and thermal fluctuations are fundamentally the same thing [10].

A concrete realisation of this point of view may be obtained on the basis of the pilot-wave formulation of quantum theory, due to de Broglie and Bohm [1–7, 11–17]. The details of the de Broglie-Bohm model may or may not be correct: but it has qualitative features, such as nonlocality, that are known to

[5] Shimony has referred to this peculiar state of affairs as 'peaceful coexistence' between relativity and quantum mechanics [8].

be properties of all hidden-variables theories; and it is helpful to work with a specific, well-defined theory.

In pilot-wave theory, a system with wavefunction $\psi(x,t)$ has a definite configuration $x(t)$ whose velocity is determined by the de Broglie guidance equation $\dot{x}(t) = j(x,t)/|\psi(x,t)|^2$, where j is the usual quantum probability current. Thus $\psi(x,t)$ determines the velocity $\dot{x}(t)$ at all times t. The wavefunction ψ is regarded as an objective 'guiding field' in configuration space, and satisfies the usual Schrödinger equation. The theory is fundamentally deterministic, the evolution being determined by the initial position x_0 and wavefunction $\psi_0(x)$. To recover quantum theory, it is assumed that an ensemble of systems with wavefunction $\psi_0(x)$ begins with a 'quantum equilibrium' distribution of configurations $\rho_0(x) = |\psi_0(x)|^2$ at $t = 0$ (guaranteeing $\rho(x,t) = |\psi(x,t)|^2$ for all t). In effect, the Born probability distribution is assumed as an initial condition.

But the theory actually allows one to consider arbitrary 'nonequilibrium' initial distributions $\rho_0(x) \neq |\psi_0(x)|^2$, which violate quantum theory [1–7]. The evolution of an arbitrary initial distribution is given by the continuity equation

$$\frac{\partial \rho(x,t)}{\partial t} + \nabla \cdot (\dot{x}(t)\rho(x,t)) = 0$$

(the same equation that is satisfied by $|\psi(x,t)|^2$). The equilibrium distribution $\rho = |\psi|^2$ is analogous to thermal equilibrium in classical mechanics, and may be accounted for by an H-theorem [1, 3, 5, 7]. Thus, pilot-wave theory indeed allows us to view quantum theory as merely a phenomenological description of an equilibrium state.[6]

Now, pilot-wave dynamics is fundamentally nonlocal: for instance, for two entangled particles at A and B with wavefunction $\psi(x_A, x_B, t)$, operations performed at B (such as switching on an external potential) have an instantaneous effect on the motion of the individual particle at A. But for a quantum equilibrium ensemble $\rho(x_A, x_B, t) = |\psi(x_A, x_B, t)|^2$, operations at B have no statistical effect at A: equilibrium noise washes out the nonlocality, and entanglement cannot be used for signalling at a distance. However, the nonlocality is hidden by statistical noise only in the equilibrium state: if $\rho_0(x_A, x_B) \neq |\psi_0(x_A, x_B)|^2$ at $t = 0$, changing the Hamiltonian at B generally induces an instantaneous change in the marginal distribution at A, amounting to a visible instantaneous signal at the statistical level [2].

This 'signal-locality theorem' – that in general there are instantaneous signals at the statistical level if and only if the ensemble is in quantum nonequilibrium $\rho_0 \neq |\psi_0|^2$ – is the key feature of pilot-wave theory that vindicates our general view of quantum theory.

But the essential, qualitative features of our view do not in fact depend on the details of pilot-wave theory. For it may be shown that the signal-locality

[6] Unfortunately, other authors tend to regard the Born rule as one of the postulates of pilot-wave theory. For them, the equilibrium theory *is* the theory. But this is like regarding $\rho = e^{-E/kT}/Z$ as a postulate of classical mechanics. To consider pilot-wave theory only in quantum equilibrium is as arbitrary as it would be to consider classical mechanics only in thermal equilibrium.

theorem is a property of *any* deterministic hidden-variables theory [18, 19]. Thus, even if pilot-wave dynamics is wrong, one can still assert – in the context of any deterministic hidden-variables theory – that quantum theory is merely the theory of a special equilibrium state in which nonlocality happens to be masked by statistical noise.

Our working hypothesis, then, is that $\rho = |\psi|^2$ is an equilibrium distribution, analogous to thermal equilibrium in classical mechanics. This state has special properties – in particular locality and uncertainty – which are not fundamental. If one accepts this idea, it becomes clear that a lot of new physics must be hidden behind quantum equilibrium noise, physics that is unavailable to us only because we happen to be trapped in an equilibrium state.

It might be thought that this new physics is not worth exploring, because it will be forever inaccessible anyway. But this is not necessarily the case. If the universe began in a nonequilibrium state $\rho \neq |\psi|^2$, this could have observable consequences in at least two ways. First, in theories of cosmological inflation, early corrections to quantum fluctuations would change the spectrum of primordial density perturbations imprinted on the cosmic microwave background; this could induce an otherwise unexpected non-Gaussianity in the statistics of temperature fluctuations over the microwave sky [6, 7]. Second, relic cosmological particles that decoupled at sufficiently early times might still be in quantum nonequilibrium today; in other words, particles left over from the early universe might violate quantum mechanics [3–7].

The second possibility is particularly relevant here. Today, there could exist matter left over from a time when the universe was still in quantum nonequilibrium. Experiments are under way searching for cosmological dark matter, which is often assumed to be made of relic particles from early times. If such particles are found, they or their decay products could be tested to see if they obey the Born rule $\rho = |\psi|^2$: for instance, in principle one might perform a single-particle two-slit interference experiment, and search for an anomalous blurring of the quantum interference pattern [3–7].

Given the possibility, then, that matter might one day be found in a state of quantum nonequilibrium $\rho \neq |\psi|^2$, let us now consider: what could one do with it? Since thermal and chemical nonequilibrium are known to have myriad technological applications, it is to be expected that quantum nonequilibrium would also be extremely useful.

2 Detection and Use of Quantum Nonequilibrium

First of all, we need to consider how one might go about deducing the distribution $\rho \neq |\psi|^2$ of nonequilibrium relic particles by statistical analysis of a random sample [7]. This is rather trivial, but perhaps worth outlining in this unusual context.

As a purely illustrative example, consider a large number N of Hydrogen

atoms in the ground state $\psi_{100}(r)$. For definiteness, let us assume that they make up a cloud of gas somewhere in space. Because the phase of the wavefunction has vanishing gradient, the de Broglie-Bohm velocity field vanishes, and pilot-wave theory predicts that each electron is at rest relative to its nucleus, at some distance r. We therefore have a static distribution $\rho(r)$, which may or may not be equal to the equilibrium distribution

$$\rho_{eq}(r) = |\psi_{100}(r)|^2 = \frac{1}{\pi a_0^3} e^{-2r/a_0}$$

predicted by quantum mechanics. To test this, one could draw a random sample of N' atoms from the cloud ($N' << N$), and measure the electron positions. The sample $r_1,\ r_2,\ r_3, ...,\ r_{N'}$ may then be used to make statistical inferences about the parent distribution $\rho(r)$. In particular, one may estimate the likelihood that $\rho(r) = \rho_{eq}(r)$. Should one deduce that, almost certainly, the cloud as a whole has a nonequilibrium distribution $\rho(r) \neq \rho_{eq}(r)$, the rest of the cloud may then be used as a resource for new physics.

For example, one could test $\rho(r)$ via the sample mean

$$\bar{r} \equiv \frac{1}{N'} \sum_{i=1}^{N'} r_i$$

If $\rho(r)$ has mean μ and variance σ^2, the central limit theorem tells us that for large N' the random variable $\bar{r}$ has an approximately normal distribution with mean μ and variance σ^2/N'. We can then calculate the probability that $\bar{r}$ differs from μ, and we can test the hypothesis that $\rho(r) = \rho_{eq}(r)$ with $\mu = \mu_{eq} = \frac{3}{2}a_0$. A standard technique is to compare the probability $P(\bar{r}|\rho_{eq})$ of obtaining $\bar{r}$ from a distribution ρ_{eq} with the probability $P(\bar{r}|\rho_{noneq})$ of obtaining $\bar{r}$ from some nonequilibrium distribution ρ_{noneq}. One usually refers to $P(\bar{r}|\rho_{eq})$ and $P(\bar{r}|\rho_{noneq})$ as the 'likelihoods' of ρ_{eq} and ρ_{noneq} respectively, given the sample mean $\bar{r}$. If $P(\bar{r}|\rho_{eq}) << P(\bar{r}|\rho_{noneq})$, one concludes that nonequilibrium is much more likely.

Similarly, using standard techniques such as the chi-square test, one may deduce the most likely form of the parent distribution $\rho(r)$, which almost certainly applies to the rest of the cloud.

Note that the same reasoning goes through even if the parent distribution is time-dependent: if the sampling is done at some time t_0, and statistical analysis favours some distribution $\rho(r, t_0)$ at time t_0, then the most likely distribution at later times may be calculated, using the continuity equation of pilot-wave dynamics.

In what follows, then, we shall assume that at time $t = 0$ we are in possession of a large number of particles with the same known wavefunction $\psi_0(x)$, and with positions x that have a known nonequilibrium distribution $\rho_0(x) \neq |\psi_0(x)|^2$.

3 Instantaneous Signalling

The most obvious application of such 'non-quantum' matter would be for instantaneous signalling across space [7].

Suppose we take pairs of our nonequilibrium particles and prepare each pair in an entangled state $\psi(x_A, x_B, t_0)$ at time t_0 (for example by briefly switching on an interaction). Given the details of the preparation process, we may use the Schrödinger equation to calculate the evolution of the wavefunction of each pair, from $\psi(x_A, x_B, 0) = \psi_0(x_A)\psi_0(x_B)$ at $t = 0$ to $\psi(x_A, x_B, t_0)$ at $t = t_0$. We then know the de Broglie-Bohm velocity field throughout the time interval $(0, t_0)$, and so we may use the continuity equation to calculate the evolution of the joint distribution for the pairs from $\rho(x_A, x_B, 0) = \rho_0(x_A)\rho_0(x_B)$ at $t = 0$ to $\rho(x_A, x_B, t_0) \neq |\psi(x_A, x_B, t_0)|^2$ at $t = t_0$.[7]

We then have the situation discussed in detail elsewhere [2]. The marginal distribution

$$\rho_A(x_A, t_0) \equiv \int dx_B \, \rho(x_A, x_B, t_0)$$

at A is known, and its subsequent evolution will depend instantaneously on perturbations applied at B, however remote B may be from A. Thus instantaneous signals may be sent from B to A.

It might be thought that superluminal signals would necessarily lead to causal paradoxes. However, it could well be that at the hidden-variable level there is a preferred slicing of spacetime, labelled by a time parameter that defines a fundamental causal sequence [20, 3, 7]. In fact in pilot-wave dynamics, which is based on velocities, the natural kinematics does define a spacetime with an inbuilt preferred state of rest – 'Aristotelian' spacetime $E \times E^3$ [21]. And in pilot-wave field theory on $E \times E^3$ [3, 4, 6, 7, 20], the above signalling procedure would allow us to define (operationally) an absolute simultaneity across space: if clocks were synchronised by this means, the speed of light would be measured to be isotropic only in the preferred rest frame; and 'backwards-in-time' effects generated by a Lorentz transformation would be wholly fictitious, merely reflecting the fact that moving clocks are incorrectly synchronised if one mistakenly assumes (with Einstein) the isotropy of the speed of light in all frames [20, 3, 7].[8]

4 Subquantum Measurement

Let us now consider how our nonequilibrium particles could be used to transcend quantum measurement theory [7].

[7] Assuming that the velocity field does not vary too rapidly in configuration space, and that the time interval $(0, t_0)$ is not inordinately long, relaxation to equilibrium will not be significant.

[8] Alternatively, one might try to develop a theory of nonlocal interactions on Minkowski spacetime. The interactions could, for example, be instantaneous in the centre-of-mass frame – a manifestly Lorentz-covariant statement. But then one must somehow make sense of backwards-in-time signals in other frames.

Nonequilibrium matter could be used to perform novel measurements on ordinary, equilibrium systems. Assume once again that we have an ensemble of what we shall now call 'apparatus' particles with known wavefunction $g_0(y)$ and known *nonequilibrium* distribution $\pi_0(y) \neq |g_0(y)|^2$. (The position y may be regarded as a 'pointer' position.) And let us now use them to measure the positions of ordinary 'system' particles with known wavefunction $\psi_0(x)$ and known *equilibrium* distribution $\rho_0(x) = |\psi_0(x)|^2$.

We shall see that, if the apparatus distribution $\pi_0(y)$ were arbitrarily narrow, one could measure the system position x_0 without disturbing the system wavefunction $\psi_0(x)$, to arbitrary accuracy, in complete violation of the uncertainty principle.

It will be convenient to illustrate the idea with a simple, exactly-solvable model. At $t = 0$, we take a system particle and an apparatus particle and switch on an interaction between them described by the Hamiltonian

$$\hat{H} = a\hat{x}\hat{p}_y$$

where a is a coupling constant and p_y is the momentum canonically conjugate to y. (This is just the standard interaction Hamiltonian used to describe an ideal quantum measurement of x using the pointer y.) For simplicity, let us neglect the Hamiltonians of x and y themselves.[9]

We then have the Schrödinger equation (for $t > 0$)

$$\frac{\partial \Psi(x,y,t)}{\partial t} = -ax\frac{\partial \Psi(x,y,t)}{\partial y}$$

for the evolution of the joint wavefunction $\Psi(x, y, t)$. This implies a continuity equation for $|\Psi(x,y,t)|^2$

$$\frac{\partial |\Psi(x,y,t)|^2}{\partial t} + ax\frac{\partial |\Psi(x,y,t)|^2}{\partial y} = 0$$

The hidden-variable velocity fields $\dot{x}$ and $\dot{y}$ must satisfy

$$\frac{\partial |\Psi(x,y,t)|^2}{\partial t} + \frac{\partial \left(|\Psi(x,y,t)|^2 \dot{x}\right)}{\partial x} + \frac{\partial \left(|\Psi(x,y,t)|^2 \dot{y}\right)}{\partial y} = 0$$

from which we may deduce the (non-standard) guidance equations[10]

$$\dot{x} = 0, \quad \dot{y} = ax$$

and the de Broglie-Bohm trajectories

$$x(t) = x_0, \quad y(t) = y_0 + ax_0 t$$

[9] This might be justified by assuming a to be relatively large; or, one can just accept the above Hamiltonian as a simple illustrative model.

[10] For standard Hamiltonians, the de Broglie guidance equation $\dot{x} = j/|\psi|^2$ usually takes the form $\dot{x} = \nabla S/m$ where S is the phase of ψ. The velocity field here is unusual because the Hamiltonian is.

Now the initial product wavefunction $\Psi_0(x,y) = \psi_0(x)g_0(y)$ evolves into the entangled wavefunction

$$\Psi(x,y,t) = \psi_0(x)g_0(y-axt)$$

In the limit $at \to 0$, we have

$$\Psi(x,y,t) \approx \psi_0(x)g_0(y)$$

and the system wavefunction $\psi_0(x)$ is undisturbed. Yet, no matter how small at may be, at the hidden-variable level the 'pointer' position $y(t) = y_0 + ax_0t$ contains information about the value of x_0 (and of $x(t) = x_0$). And this 'sub-quantum' information about x will be visible to us if the pointer distribution $\pi_0(y)$ is sufficiently narrow.

For consider an ensemble of similar experiments, where x and y have the initial joint distribution

$$P_0(x,y) = |\psi_0(x)|^2 \pi_0(y)$$

(equilibrium for x and nonequilibrium for y). The continuity equation

$$\frac{\partial P(x,y,t)}{\partial t} + ax\frac{\partial P(x,y,t)}{\partial y} = 0$$

implies that at later times

$$P(x,y,t) = |\psi_0(x)|^2 \pi_0(y-axt)$$

If $\pi_0(y)$ is localised – say $\pi_0(y) \approx 0$ for $|y| > w/2$ – then $P(x,y,t) \neq 0$ only if $x \in \left(\frac{y}{at} - \frac{w}{2at}, \frac{y}{at} + \frac{w}{2at}\right)$. If we measure y by standard methods, we may then deduce that x lies in the interval $\left(\frac{y}{at} - \frac{w}{2at}, \frac{y}{at} + \frac{w}{2at}\right)$, where the error margin $\frac{w}{2at} \to 0$ as the width $w \to 0$.

Thus, if the nonequilibrium distribution has an arbitrarily small width w, then to arbitrary accuracy we may measure the position x of each equilibrium particle without disturbing the wavefunction $\psi_0(x)$.

We have considered the extreme case where $\pi_0(y)$ is arbitrarily narrow. For a finite width $w < \Delta$, where Δ is the width of $|g_0(y)|^2$, one obtains an improvement over quantum measurements, in the sense that one may make probabilistic statements about the value of x that convey more information than quantum theory allows; while if $w > \Delta$, the measurements will be less accurate than those of quantum theory [7].

We have for simplicity considered an exactly-solvable system with a total Hamiltonian that is rather unusual. But similar conclusions would be arrived at for more standard systems. The key point is simply that, if the interaction between two variables x and y is sufficiently weak, then while the wavefunction of x is hardly disturbed, nevertheless at the hidden-variable level the value of y contains information about x; and if y has a sufficiently narrow nonequilibrium distribution this information will be visible to us.

Generalising, if the width w of the nonequilibrium 'apparatus' distribution is arbitrarily small, then by a sequence of measurements of the form just described, it is clear that for a system particle with arbitrary wavefunction $\psi(x,t)$ one can determine the hidden-variable particle trajectory $x(t)$ without disturbing $\psi(x,t)$, to arbitrary accuracy.

5 Distinguishing Non-Orthogonal Quantum States without Disturbing them

It is a theorem of quantum mechanics that non-orthogonal states cannot be distinguished without disturbing them [22]. (To find out which of two states $|\psi_1\rangle$ or $|\psi_2\rangle$ a given system is in without disturbing them, one may let the system interact with an ancillary system in a known initial state $|u\rangle$, such that the joint system evolves as $\hat{U}\left(|\psi_1\rangle\,|u\rangle\right) = |\psi_1\rangle\,|v\rangle$ and $\hat{U}\left(|\psi_2\rangle\,|u\rangle\right) = |\psi_2\rangle\,|v'\rangle$. One would hope that $|v\rangle$ and $|v'\rangle$ are different, so that a measurement of the ancillary system would distinguish $|\psi_1\rangle$ from $|\psi_2\rangle$. However, because inner products are preserved by unitary evolution, it must be that $\langle v|v'\rangle\langle\psi_1|\psi_2\rangle = \langle\psi_1|\psi_2\rangle$: if $\langle\psi_1|\psi_2\rangle \neq 0$ then $\langle v|v'\rangle = 1$ and the required information cannot be obtained from the state of the ancillary system. Thus, to distinguish between $|\psi_1\rangle$ and $|\psi_2\rangle$, at least one of them must be disturbed.)

This theorem breaks down if one has access to nonequilibrium matter [7]. For example, if $|\psi_1\rangle$, $|\psi_2\rangle$ are distinct initial states of a single spinless particle, then in de Broglie-Bohm theory the velocity fields $j_1(x,t)/\left|\psi_1(x,t)\right|^2$, $j_2(x,t)/\left|\psi_2(x,t)\right|^2$ generated by the wavefunctions $\psi_1(x,t)$, $\psi_2(x,t)$ will in general be different, even if $\langle\psi_1|\psi_2\rangle = \int dx\ \psi_1^*(x,0)\psi_2(x,0) \neq 0$. The hidden-variable trajectories $x_1(t)$ and $x_2(t)$ – associated with $\psi_1(x,t)$ and $\psi_2(x,t)$ respectively – will generally differ if $\psi_1(x,0) \neq \psi_2(x,0)$ (even if $x_1(0) = x_2(0)$).

Thus, a subquantum measurement of the particle trajectory (even over a short time) would enable one to distinguish the quantum states $|\psi_1\rangle$ and $|\psi_2\rangle$ without disturbing them, to arbitrary accuracy.

6 Eavesdropping on Quantum Key Distribution

By using nonequilibrium matter to perform subquantum measurements, one could also secretly eavesdrop on the distribution of quantum cryptographic keys [7].

A central technique of quantum cryptography is quantum key distribution. Two parties – 'Alice' and 'Bob' – want to share a sequence of bits that will be used for cryptographic operations. This sequence or 'key' must be unknown to anyone else: any attempt by a third party ('Eve') to eavesdrop while the key is being distributed must be detectable by Alice and Bob.

The bits are generated by a random choice of quantum states and/or the random outcomes of quantum measurements. Three protocols for quantum key distribution are known to be secure against classical or quantum attacks (that

is, against eavesdropping based on classical or quantum physics): BB84 due to Bennett and Brassard [23], B92 due to Bennett [24], and E91 or EPR due to Ekert [25].[11] But these protocols are *not* secure against a 'subquantum' attack by an eavesdropper who possesses non-quantum or nonequilibrium matter (with a distribution narrower than the wavefunction width).

6.1 Breaking the BB84 and B92 Protocols

Consider first the BB84 and B92 protocols. Both rely on the impossibility of distinguishing non-orthogonal quantum states without disturbing them.

In BB84, Alice sends a random sequence of spin-1/2 states $|+z\rangle$, $|-z\rangle$, $|+x\rangle$, $|-x\rangle$ to Bob, who randomly measures $\hat{\sigma}_z$ or $\hat{\sigma}_x$. In each instance, they publicly announce whether Alice sent an eigenstate of $\hat{\sigma}_z$ or $\hat{\sigma}_x$ (but not which eigenvalue) and whether Bob measured $\hat{\sigma}_z$ or $\hat{\sigma}_x$ (but not the results). They discard instances where their choices of $\hat{\sigma}_z$ or $\hat{\sigma}_x$ differed. Finally, they test a random sample of the remaining data: there should be strict agreement between the eigenvalues sent by Alice and the measurement results obtained by Bob, if and only if there was no eavesdropping (that is, no disturbance of the states sent by Alice).

B92 is similar. Alice sends a random sequence of non-orthogonal states $|u_0\rangle$, $|u_1\rangle$ ($\langle u_0|u_1\rangle \neq 0$) to Bob, who randomly measures $\hat{P}_0 = 1 - |u_1\rangle\langle u_1|$ or $\hat{P}_1 = 1 - |u_0\rangle\langle u_0|$. Bob publicly tells Alice which of his results are positive (but not which of $\hat{P}_0$, $\hat{P}_1$ was measured); the other instances are discarded. If there is no eavesdropping, the remaining instances will be perfectly correlated (with respect to the labels 0 and 1), and again this can be checked for a random sample.

Now, if Eve possesses non-quantum matter with an arbitrarily narrow nonequilibrium distribution, she may identify the states sent by Alice without disturbing them. For example, in the case of B92 $|u_0\rangle$ and $|u_1\rangle$ could be states of a spinless particle with wavefunctions $\psi_0(x,t)$ and $\psi_1(x,t)$: as we have pointed out, by monitoring the hidden-variable trajectories Eve would be able to distinguish the wavefunctions without disturbing them, to arbitrary accuracy. Eve would then know the bit sequence making up the supposedly secret key shared by Alice and Bob.

Similarly, in the case of BB84, Eve could identify the states sent by Alice, again without disturbing them, thereby obtaining the key. (Though here, for spin-1/2 states one must consider pilot-wave theory for two-component wavefunctions [7, 13].)

6.2 Breaking the E91 or EPR Protocol

From a hidden-variables perspective, the protocol formulated by Ekert is particularly interesting. For Ekert's scheme relies on the completeness of quantum

[11] For a review of security proofs, and of quantum cryptography generally, see Gisin *et al.* [26].

theory – that is, on the assumption that there are no hidden 'elements of reality'.

In the case of E91, pairs of spin-1/2 particles in the singlet state are shared by Alice and Bob, who perform measurements along random axes (say along either x or z). They publicly announce which axes were used in each instance, but not the results. Instances where the axes differ are discarded. If there is no eavesdropping, the remaining instances will be perfectly (anti-)correlated.

From the point of view of standard quantum theory, as Ekert puts it: 'The eavesdropper cannot elicit any information from the particles while in transit ..... because there is no information encoded there. The information "comes into being" only after the legitimate users perform measurements ..... as long as quantum theory is not refuted as a complete theory the system is secure' [25].

But our Eve does have access to information outside the domain of quantum theory. In particular, she can measure the particle positions while in transit, without disturbing the wavefunction, and thereby *predict* the outcomes of spin measurements at the two wings (for the publicly-announced axes).[12] Thus Eve is able to predict the key generated at both wings.

7 Reading all the Results of a Parallel Quantum Computation

As noted in particular by Deutsch [27], quantum theory allows parallel Turing-type computations to occur in different branches of the state vector for a single computer. However, owing to the effective collapse that occurs under measurement, an experimenter is able to access only one result; the outputs of the other computations are lost. Of course, by clever use of entanglement and interference, one can make quantum computation remarkably efficient for certain special problems. But it is fair to say that, in general, what at first sight would seem to be a massive increase in computational power due to quantum parallelism is not, in fact, realised in practice.

Here we show that *all* the results of a parallel quantum computation could be read by an experimenter in possession of a store of nonequilibrium matter with a very narrow distribution.

Consider, for example, a single spinless particle with Hamiltonian $\hat{H} = \hat{p}^2/2 + V(\hat{x})$ and wavefunction $\psi(x,t)$ (where the mass $m = 1$ and $\hbar = 1$). The particle trajectory $x(t)$ is determined by the standard de Broglie relation

$$\dot{x}(t) = \frac{j}{|\psi|^2} = \mathrm{Im}\left(\frac{1}{\psi}\frac{\partial\psi}{\partial x}\right)$$

Let the wavefunction be a superposition of N energy eigenfunctions

$$\psi(x,t) = \sum_{n\in S} \phi_n(x) e^{-iE_n t}$$

[12] In the pilot-wave theory of spin-1/2 as formulated by Bell [13], the hidden-variable particle positions within the wavepacket determine the outcomes of Stern-Gerlach spin measurements.

where S is a set of N quantum numbers (for example $S = \{15,\ 231,\ 2891,\ .....\}$). We assume that the $\phi_n(x)$ are known functions – obtained by solving the eigenvalue problem $\hat{H}\phi_n(x) = E_n\phi_n(x)$ – but that the values of n actually present in the superposition are not known.

The quantum numbers $n \in S$ could encode the results of computations. They could each represent the end result of a long and complex Turing-like computation, one taking place in each branch of the state vector for the computer. One can imagine the final output of each computation being encoded in the energy eigenvalue of a single particle (a component of the computer).

Now in standard quantum theory, a measurement of the energy of the particle will yield just one of the eigenvalues E_n. To find out what other eigenvalues are present in the superposition, one would have to run the whole computation many times – to produce an ensemble of copies of the same wavefunction – and repeat the energy measurement for each. But then one may as well just run many different computations on a single classical computer, one after the other.

However, provided the eigenfunctions $\phi_n(x)$ overlap in space, the hidden-variable trajectory $x(t)$ contains information about all the modes present in the superposition. If we were in possession of nonequilibrium matter with a very narrow distribution, we would be able to measure $x(t)$ without disturbing the wavefunction $\psi(x,t)$. We could then 'read' the set S of quantum numbers and so obtain the results of all the parallel computations, even though the computer has been run only once [3, 7].

Let us illustrate this with a simple, concrete example. For a particle in a one-dimensional box of length π, we have eigenfunctions $\phi_n(x) = \sqrt{\frac{2}{\pi}}\sin nx$ and eigenvalues $E_n = \frac{1}{2}n^2$ ($n = 1,\ 2,\ 3,\ ....$). In the case of $N = 2$ unknown energy levels $E_a,\ E_b$ we have

$$\begin{aligned}\psi(x,t) &= \frac{1}{\sqrt{2}}\left(\phi_a(x)e^{-iE_at} + \phi_b(x)e^{-iE_bt}\right)\\ &= \frac{1}{\sqrt{\pi}}\left(\sin ax\, e^{-i\frac{1}{2}a^2t} + \sin bx\, e^{-i\frac{1}{2}b^2t}\right)\end{aligned}$$

and

$$\dot{x}(t) = \frac{(b\sin ax\cos bx - a\sin bx\cos ax)\sin\frac{1}{2}\left(a^2-b^2\right)t}{\sin^2 ax + \sin^2 bx + 2\sin ax\sin bx\cos\frac{1}{2}\left(a^2-b^2\right)t}$$

If we knew the values of $x(t),\ \dot{x}(t)$ at two distinct times $t = t_1,\ t_2$, the last equation could be solved for the quantum numbers $a,\ b$. This might be realised by performing subquantum measurements of $x(t)$ at four times $t = t_1,\ t_1 + \epsilon,\ t_2,\ t_2 + \epsilon$ (with ϵ very small).

More generally, for a superposition of N eigenfunctions, given N pairs of values $x(t_i),\ \dot{x}(t_i)$ at N times $t_1,\ t_2,\ ....,\ t_N$ the de Broglie equations may be solved for the N quantum numbers n, thus yielding the results of all N parallel computations.

8 Conclusion

We have argued that immense physical resources are hidden from us by quantum noise, and that we will be unable to access those resources only for as long as we are trapped in the 'quantum heat death' – a state in which all systems are subject to the noise associated with the Born probability distribution $\rho = |\psi|^2$.

It is clear that hidden-variables theories offer a radically different perspective on quantum information theory. In such theories, a huge amount of 'subquantum information' is currently hidden from us by virtue of the fact that we happen to live in a time and place where the hidden variables have a certain 'equilibrium' distribution. As we have mentioned, nonequilibrium instantaneous signals occur not only in pilot-wave theory but in *any* deterministic hidden-variables theory [18, 19]. And in pilot-wave theory at least, we have shown that the security of quantum cryptography depends on our being trapped in quantum equilibrium; and, that out of equilibrium the full power of quantum parallelism would be accessible for computational purposes.

Some might prefer to regard this work as showing how the principles of quantum information theory depend crucially on a particular axiom of quantum theory – specifically, the Born rule $\rho = |\psi|^2$.[13]

On the other hand, if one takes hidden-variables theories seriously as physical theories of Nature, one can hardly escape the conclusion that we just happen to be confined to a particular state in which our powers are limited by an all-pervading statistical noise. It then seems important to search for violations $\rho \neq |\psi|^2$ of the Born rule, in particular for particles from the early universe [3–7].

Acknowledgement. This work was supported by the Jesse Phillips Foundation.

REFERENCES

[1] A. Valentini, Phys. Lett. A **156**, 5 (1991).

[2] A. Valentini, Phys. Lett. A **158**, 1 (1991).

[3] A. Valentini, PhD thesis, International School for Advanced Studies, Trieste, Italy (1992).

[4] A. Valentini, in *Bohmian Mechanics and Quantum Theory: an Appraisal*, eds. J. T. Cushing *et al.* (Kluwer, Dordrecht, 1996).

[5] A. Valentini, in *Chance in Physics: Foundations and Perspectives*, eds. J. Bricmont *et al.* (Springer, Berlin, 2001) [quant-ph/0104067].

[6] A. Valentini, Int. J. Mod. Phys. A (forthcoming).

[7] A. Valentini, *Pilot-Wave Theory of Physics and Cosmology* (Cambridge University Press, Cambridge, forthcoming).

[8] A. Shimony, in *Foundations of Quantum Mechanics in the Light of New Technology*, ed. S. Kamefuchi (Physical Society of Japan, Tokyo, 1984).

[9] D. W. Sciama, P. Candelas and D. Deutsch, Adv. Phys. **30**, 327 (1981).

[13] One might also consider, for example, the role of the axiom of linear evolution of quantum states [28, 29].

[10] L. Smolin, Class. Quantum Grav. **3**, 347 (1986).

[11] L. de Broglie, in *Électrons et Photons: Rapports et Discussions du Cinquième Conseil de Physique*, ed. J. Bordet (Gauthier-Villars, Paris, 1928). [English translation: G. Bacciagaluppi and A. Valentini, *Electrons and Photons: The Proceedings of the Fifth Solvay Congress* (Cambridge University Press, Cambridge, forthcoming).]

[12] D. Bohm, Phys. Rev. **85**, 166; 180 (1952).

[13] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, 1987).

[14] P. Holland, *The Quantum Theory of Motion: an Account of the de Broglie-Bohm Causal Interpretation of Quantum Mechanics* (Cambridge University Press, Cambridge, 1993).

[15] D. Bohm and B. J. Hiley, *The Undivided Universe: an Ontological Interpretation of Quantum Theory* (Routledge, London, 1993).

[16] J. T. Cushing, *Quantum Mechanics: Historical Contingency and the Copenhagen Hegemony* (University of Chicago Press, Chicago, 1994).

[17] *Bohmian Mechanics and Quantum Theory: an Appraisal*, eds. J. T. Cushing *et al.* (Kluwer, Dordrecht, 1996).

[18] A. Valentini, quant-ph/0106098.

[19] A. Valentini, in *Modality, Probability, and Bell's Theorems*, eds. T. Placek and J. Butterfield (Kluwer, Dordrecht, 2002) [quant-ph/0112151].

[20] D. Bohm and B. J. Hiley, Found. Phys. **14**, 255 (1984).

[21] A. Valentini, Phys. Lett. A **228**, 215 (1997).

[22] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[23] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984).

[24] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[25] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[26] N. Gisin *et al.*, Rev. Mod. Phys. (forthcoming) [quant-ph/0101098].

[27] D. Deutsch, Proc. Roy. Soc. London A **400**, 975 (1985).

[28] A. Valentini, Phys. Rev. A **42**, 639 (1990).

[29] D. S. Abrams and S. Lloyd, Phys. Rev. Lett. **81**, 3992 (1998).